AWIPS SYSTEM ADMINISTRATION NOTE 3 (for Electronics Systems Analysts)
Engineering Division
W/OSO32: LTB

SUBJECT : Advanced Weather Interactive Processing System (AWIPS) System Passwords Maintenance

PURPOSE : Provide guidelines for AWIPS system passwords with emphases on the importance of monitoring and periodically changing the passwords.

BACKGROUND

The AWIPS System Administrator at each AWIPS site is responsible for AWIPS security. AWIPS is critical to the National Weather Service (NWS) operations. The AWIPS Security Policy focuses on the following key aspects of computer security:

- To prevent use of all AWIPS computers, network, and communications resources by unauthorized persons.

- To prevent unauthorized actions that may be caused by individuals who gain access to AWIPS computers or networks.

- To protect the confidentiality of sensitive information by denying access to unauthorized persons.

A common thread in these security goals is to ensure that unauthorized persons do not gain access to AWIPS computers and networks. AWIPS system passwords are the primary security controls that enforce the AWIPS security policy. However, passwords are effective only if they are monitored and maintained rigorously.

In particular, this note addresses the following key items:

- General guidelines for passwords.

- Guidelines for maintaining passwords.

- The need to assign a password for the 'fxa' user.

- The need to change passwords routinely.

- The need to create new user accounts to handle specific needs such as remote access from the National Weather Service Headquarters (WSH) for gathering information from sites.

Consult the procedures section of this note for specific steps to perform the various types of password assignments and maintenance activities.

GUIDELINES

Each AWIPS site has a number of network computers, data/application servers, graphic workstations, text workstations, communication processors, and routers. Nearly all of these systems have some form of user accounts with corresponding passwords. There is the conventional UNIX root user (the super user) on each computer, and many AWIPS-specific user accounts such as awipsusr, fxa, ncfuser, oper, textdemo, freeway and firetest.

The chosen password for a user account must be difficult to guess. Examples of easily guessed passwords are: names of any kind (first, last, or middle), social security numbers, birth dates, words from the dictionary, strings composed of all digits or letters repeating in pattern, and strings less than six characters long. A difficult-to-guess password forces an intruder to attempt a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort can take, on the average, more than 100 years to complete.

Guidelines for Password Selection:

The following guidelines apply to passwords chosen for any AWIPS user account:

- Select a password that is at least six characters long.
- Pick “words” that are not in any dictionary; mix alpha numeric characters and special symbols.
- Use mixed-case alphabets in passwords.
- Include one or more digits and punctuation marks in the password. For example, a good password is two easily remembered but unrelated words joined by a punctuation character.
- Select a password that can be remembered by the user and does not need to be written down.
- Select a password that can be quickly typed without having to look at the keyboard. This makes it harder for any bystander to observe the password by watching someone type it.

Guidelines for Password Maintenance

Passwords can be effective only if they are monitored and maintained by following these general guidelines:

- Periodically check for any user accounts without a password.
- Change all passwords at least quarterly or when personnel changes occur.

- Change all passwords after installation of new software or hardware.

- Choose a completely new password every time the password has to be changed.

Guidelines for Root Password

Safeguarding the root password is crucial because it is the superuser who has access to all AWIPS computer and network resources. Besides the AWIPS site’s system administrator, the Network Control Facility (NCF) must have the root password. When anyone outside of the NCF needs access to the root password, for example, (selected members of the AWIPS development team may need such access to fix a software problem), the site should do the following:

- Confirm the requested root access with the site security manager.

- Send an electronic mail notification to the AWIPS security manager mentioning that the root access is being granted to a person outside of the NCF.

- Change the root password.

- Provide the password to the NCF and the person who temporarily needs root access.

- Once the work is complete, change the root password again and provide the NCF with the new root password.

Password Guidelines for ‘fxa’ Users

Stopping and starting the NEXRAD data acquisition on AWIPS requires the site personnel to be user 'fxa.' The AWIPS configuration typically has the password for 'fxa' disabled. Since 'fxa' does not have a password, the operator must log in as **root** and use the **su fxa** command to assume the role of the 'fxa' user. This results in the root password being given to any site personnel who must start or stop the NEXRAD data acquisition.

To avoid distributing the root password widely and potentially compromising the password, the site system administrator should establish a password for user ‘fxa.’ The procedures section shows how to assign a password for the 'fxa' user.

Guidelines for Additional AWIPS User Accounts

To support specific NWS objectives, it may be necessary for users from WSH or regional offices to gain access to a site's computers. For example, headquarters personnel may need to access the data acquisition logs to monitor the products availability or assess the timeliness of product distribution. When such remote access is needed, the site system administrator should follow these guidelines:

- Require that any new user account request be submitted formally through the AWIPS Security Manager.

- Verify with the Site's Security Manager before creating a new user account.

- Create the new user account with a temporary password; communicate the password to the user, and ask them to login and change the password immediately.

- Delete the account when no longer needed.

PROCEDURES:

The following sections outline the procedures for various password maintenance tasks. Where applicable, the procedures point to specific AWIPS documentation.

Procedures for Assigning Passwords to 'fxa' Users

To assign a password to the 'fxa' user, follow these steps:

1. Log in as root on the DS1.
2. Start SAM.
3. Double-click on the Accounts for Users and Groups icon.
4. Double-click on NIS users.
5. Click on users ‘fxa’ and select Action/Modify.
6. In the “Modify a User” window, select modify password.
7. Establish a password and exit.

SAM will update the NIS password to all servers and workstations.

Consult the AWIPS System Manager's Manual for further details.

Procedures for Creating New User Accounts

Consult Chapter 3 of the AWIPS System Manager's Manual for detailed information on adding a new user account using SAM.

John McNulty
Chief, Engineering Division